REMARKS

The present amendment is responsive to the Non-final Office Action mailed June 29, 2007. Following entry of the foregoing amendments, Claims 1-12, 14-25, and 27-55 remain pending in this application. Independent Claims 1, 14, 27, 33, 34, 35, 40, and 47, and dependent Claims 9, 11, 22, and 54 have been amended by the present Response. Dependent Claims 13, 26 have been cancelled. Applicant respectfully submits that no new matter has been added by the foregoing amendments. Reconsideration of the application, as amended, is requested.

Applicant would like to thank Examiner Smithers for the Telephonic Examiner's Interview that was conducted on September 10, 2007. In the Interview, patentable distinctions between the claimed invention and the cited art of record were discussed. In particular, it was discussed that the cited art of record does not teach or suggest encrypting plaintext by utilizing a non-linear device and by performing a wavelet transform on the plaintext to produce cyphertext, as recited by each of the independent claims.

Rejection of Claims 1-55 Under 35 U.S.C. § 102(e)

In the Non-final Office Action, Claims 1-55 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,898,756 to *Fekri* ("*Fekri*"). However, the Applicant respectfully contends that the amended claims are patentable over *Fekri*.

Patentability of the Amended Independent Claims

As discussed in the Telephonic Examiner's Interview, *Fekri* does not teach or suggest "an encryption system that includes at least one non-linear device and is operable to receive plaintext and perform an inverse wavelet transformation (or wavelet transformation) over a finite field on said plaintext to produce cyphertext," as recited by amended independent Claim 1.

Although *Fekri* relates to systems and methods for enabling efficient error correction and encryption using wavelet transforms over finite fields (See *Fekri* at Abstract), *Fekri* does not teach or suggest the use of at least one non-linear device in order to encrypt plaintext. There is no discussion of non-linear devices anywhere in *Fekri*. *Fekri* does recite non-linear code data in

dependent Claims 3, 17, 35, and 57; however, the non-linear code data recited in the dependent claims of *Fekri* does not teach or suggest the use of at least one non-linear device for encrypting plaintext. Instead, the non-linear code data of *Fekri* is a type of data that may be encoded by the systems and methods recited in *Fekri* and then checked for errors after it is transmitted.

In marked contrast to *Fekri*, amended Claim 1 recites an encryption system that "includes at least one non-linear device." The at least one non-linear device introduces non-linearity into the wavelet transformations, thereby increasing the security of the encryption. Some of the advantages of encryption systems that utilize at least one non-linear device and a wavelet or inverse wavelet transformation are discussed throughout the Specification of the present patent application. For example, paragraphs [0061] – [0063] (or the first full paragraph on page 16 through the top of page 17 of the Specification as originally filed) state in part:

> [0061] In addition to this decorrelating property of the finite-field wavelets, there are two more key properties that the present invention exploits to construct a public key encryption system. First, a high degree of non-linearity can be introduced by using nonlinear finite field wavelets. Secondly, nonlinear wavelets have a unique structure that can be exploited to construct a public key encryption system with a very large key space.
>
> [0062] … [S]ecurity is tied to the length of the wavelet basis function and to the nonlinearity within the wavelet transform.
>
> [0063] … [S]ystems of the present invention utilize wavelets that operate over GF(256) and a nonlinear device that performs a mapping of field elements to their inverse in the field. Therefore, cracking a cryptosystem of the present invention using a chosen cyphertext attack … is equivalent to solving a set of nonlinear equations over finite fields …

As another example, paragraphs [0075] – [0076] (or the first full paragraph on page 21 through the top of page 22 of the Specification as originally filed) state in part:

> [0075] … [E]ncryption and decryption systems 15, 30 of the present invention introduce nonlinearity to the wavelet transforms used to encrypt and decrypt information transmitted across the communication channel. Therefore, according to one aspect of the present invention, a nonlinear wavelet may be utilized in order to make the system resistant against security attacks. FIG. 5A shows an elementary nonlinear transform block 30 used for the encryption …
>
> [0076] As shown in FIG. 5A, nonlinearity in the transform block is introduced by taking the output y(n) of the wavelet system and passing it through a nonlinear operation 85 and adding the result to the incoming plaintext x(n) …

As clearly supported throughout the Specification, the security of an encryption system can be increased by utilizing both a wavelet transform operation and at least one non-linear device. The use of at least one non-linear device in an encryption system that performs a wavelet transform or an inverse wavelet transform is not taught or suggest by *Fekri*.

For at least the reasons set forth above, *Fekri* fails to teach or suggest an encryption system that "includes at least one non-linear device and that is operable to encrypt said plaintext at least in part by performing an inverse wavelet transformation over a finite field on said plaintext to produce cyphertext." Therefore, the Applicant respectfully asserts that amended independent Claim 1 is allowable over *Fekri*. Because Claims 2-12 depend from independent Claim 1, those claims are likewise allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features.

Independent Claims 14, 27, 34, 35, 40, and 47 have been amended in the same manner as independent Claim 1. Accordingly, amended independent Claims 14, 27, 34, 35, 40, and 47 also recite, among other things, that the encryption system "includes at least one non-linear device" and is operable to "encrypt said plaintext at least in part by performing an inverse wavelet transformation (or wavelet transformation in some of the claims) over a finite field on said

plaintext to produce cyphertext." The Applicant respectfully asserts that all remarks addressing the patentability of amended Claim 1 are also applicable to amended independent Claims 14, 27, 34, 35, 40, and 47. Therefore, the Applicant asserts that amended independent Claims 14, 27, 34, 35, 40, and 47 are allowable for the same reasons set forth above with respect to amended Claim 1. Further, because Claims 15-25, 28-33, 36-39, 41-46, and 48-55 depend from independent Claim 14, 27, 35, 40, and 47 respectively, the Applicant asserts those claims are also allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features.

Patentability of Amended Dependent Claims 9, 22, and 54

By the present amendment, dependent Claim 9 has been amendment to recite filter coefficients utilized to perform an inverse wavelet transformation that are based at least in part on a secret key. Similar amendments have been made to dependent Claims 22 and 54.

Fekri does not teach or suggest the generation or derivation of wavelet transform filter coefficient based at least in part on a secret key. In addition, these dependent claims ultimately depend from amended independent claims for which arguments of patentability have been provided above. Accordingly, Applicant respectfully asserts that amended dependent Claims 9, 22, and 54 are patentable over *Fekri* for at least the foregoing reasons.

CONCLUSION

The Applicant believes that each matter raised by the Examiner has been addressed. Allowance of the claims is respectfully solicited. It is not believed that extensions of time or fees for addition of claims are required beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR §1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 19-5029.

If there are any issues which can be resolved by telephone conference or an Examiner's Amendment, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

Rhett S. White
Attorney for Applicant
Registration No. 59,158

Date: September 19, 2007

SUTHERLAND ASBILL & BRENNAN, LLP
999 Peachtree Street, NE
Atlanta, GA 30309-3996
(404) 853-8233
(404) 853-8806 (fax)

SAB Docket No.: 17625-0050